IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANT:	Warwick Ford
APPLICATION NO.:	09/921,265
FILING DATE:	August 1, 2001
TITLE:	Authenticated Communication Using a Shared Unpredictable Secret (As Amended)
EXAMINER:	Matthew T. Henning
GROUP ART UNIT:	2131
ATTY. DKT. NO.:	21190-05339

MAIL STOP APPEAL BRIEF- PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDED APPEAL BRIEF

I. Real Party in Interest

The subject application is owned by Verisign, Inc. of Mountain View, California. Assignment from the inventors to Verisign was recorded on Jan. 8, 2002 at Reel 012438, Frame 0190.

II. Related Appeals and Interferences

There are no known related appeals or interferences that may directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims

Claims 1-8 and 10-19 stand finally rejected. Specifically, claims 1, 5-8 and 16-19 were rejected under 35 U.S.C. 102(e) as anticipated by Fielder et al. (USPN 5,995,624). Claims 1, 5-8, 11-12 and 14-19 were rejected under 35 U.S.C 103(a) as unpatentable over Fielder further in view of Menezes (Handbook of Applied Cryptography). Claims 2-4 were rejected under 35 U.S.C 103(a) as unpatentable over Fielder further in view of Yatsukawa (USPN 6,148,404). Claims 10 and 13 were rejected under 35 U.S.C 103(a) as unpatentable over the combination of Fielder and Menezes, further in view of Lamport, Leslie (Password Authentication with Insecure Communications).

Claim 9 stands as cancelled in Applicant's amendment dated May 11, 2005.

On Jan. 27, 2006, the Appellant appealed from the final rejection of claims 1-8 and 10-19. The claims on appeal are set forth in an appendix attached hereto.

IV. Status of Amendments

The Appellant has not amended the claims since the final rejection.

V. Summary of Claimed Subject Matter

In general, the claimed invention is directed to methods, systems and computer readable media containing computer program instructions for validating a client device (1) by a server device (5). In one method, a shared unpredictable secret (50) is generated (24). The shared unpredictable secret (50) is stored (25) in the client device (1) and in the server device (5). The client device (1) is required to prove (33,34) that it holds the correct shared unpredictable secret (50) as a precondition to the server device (5) validating (44) the client device (1). In addition, the shared unpredictable secret (50) is replaced (39,40) by a new shared unpredictable secret (54)

when the server device (5) validates (44) the client device (1). Specifically, the server device (5) sends (38) update data (53) to the client device (1). The client device (1) applies the update data (53) to the shared unpredictable secret (50) to generate (39) a new secret (54). The client device (1) replaces (39) the shared unpredictable secret (50) with the new secret (54). See, e.g., page 7 lines 3-4; page 8 lines 13-14; page 9 line 20 - page 11 line 24, and FIGS. 2-3.

Claim 1. With exemplar reference to FIGS. 2-3 and the corresponding text, independent claim 1 is a method for validating a client device by a server device comprising the steps of: (i) generating a shared unpredictable secret (24, page 7 lines 3-4); (ii) storing the shared unpredictable secret in the client device and in the server device (25, page 8 lines 13-14); (iii) requiring the client device to prove that it holds a correct secret as a precondition to the server device validating the client device (33, 34, page 9 line 20 – page 10 line 16); and (iv) replacing the shared unpredictable secret by a new shared unpredictable secret when the server device validates the client device (39, 40, page 11 lines 22-24, page 13 lines 14-19), wherein (a) the server device sends update data to the client device (38, page 11 lines 4-5), (b) the client device applies the update data to the shared unpredictable secret to generate a new secret (39, page 11 lines 5-7); and the client device replaces the shared unpredictable secret with the new secret (39, page 11 lines 22-24).

Claim 18. With examplar reference to FIG. 1, independent claim 18 is a system for enabling a server device to validate a client device. The system comprises (i) at least one client device (1(1)-1(n), page 3 lines 8-9); (ii) a server device (5, page 3 lines 9-13); and (iii) a shared unpredictable secret (50, page 5 lines 13-15).

With examplar reference to FIGS. 2-3, the system also includes the following means-plus-function elements (where the reference numbers indicate the disclosure of the

corresponding function): (iv) means for storing the shared unpredictable secret in the client device (25, page 8 lines 13-14); (v) means for storing the shared unpredictable secret in the server device (25, page 8 lines 13-14); (vi) coupled to the client device and to the server device, means for determining whether the client device holds a correct secret (33,34, page 9 line 20 – page 10 line 11); (vii) coupled to the determining means, means for allowing the server device to validate the client device when the client device proves that it holds a correct secret (44, page 10 lines 11-16, page 13 lines 12-14); and (viii) coupled to the client device and to the server device, means for replacing the original shared unpredictable secret with a new shared unpredictable secret when the server device validates the client device (39,40, page 11 lines 22-24, page 13 lines 14-19). Said means for replacing further comprises (a) means for the server device to send update data to the client device (38, page 11 lines 4-5); and (b) means for the client device to apply the update data to the shared unpredictable secret to generate a new secret(39, page 11, lines 5-7); and (c) means for the client device to replace the shared unpredictable secret with the new secret (39, page 11 lines 22-24).

For claim 18, an example of a structure corresponding to these various "means" can be found at page 5 line 25 – page 6 line 4. This passage explains that "[a]ll of the method steps illustrated herein describe modules that can be implemented in hardware, software, and/or firmware. Some of these modules reside on the client device 1 and some on the server device 5, as will be understood by examining the Figures in conjunction with the following description."

Claim 19. With examplar reference to FIGS. 2-3, independent claim 19 is a computer readable medium containing computer program instructions for enabling a server device to validate a client device, said computer program instructions causing the execution of the following steps: (i) generating a shared unpredictable secret (24, page 7 lines 3-4); (ii) storing

the shared unpredictable secret in the client device and in the server device (25, page 8 lines 13-14); (iii) requiring the client device to prove that it holds a correct secret as a precondition to allowing the client device to be validated by the server device (33,34, page 9 line 20 – page 10 line 16); and (iv) replacing the shared unpredictable secret by a new shared unpredictable secret when the client device is validated by the server device (39,40, page 11 lines 22-24, page 13 lines 14-19), wherein (a) the server device sends update data to the client device (38, page 11 lines 4-5); the client device applies the update data to the shared unpredictable secret to generate a new secret (39, page 11 lines 4-5); and the client device replaces the shared unpredictable secret with the new secret (39, page 11 lines 22-24). The reference numbers of the previous sentence indicate the disclosure of the corresponding function. The passage found at page 5 line 25 – page 6 line 4 explains that "[a]ll of the method steps illustrated herein describe modules that can be implemented in . . . software . . .," thereby supporting the computer readable medium aspect of claim 19.

VI. Grounds of Rejection to be Reviewed on Appeal

The ground of rejection presented for review in the instant appeal are as follows:

A. Claims 1, 5-8 and 16-19 were rejected under 35 U.S.C. § 102(e) as anticipated by Fielder (U.S. Patent No. 5,995,624).

B. Claims 1, 5-8, 11-12 and 14-19 were rejected under 35 U.S.C. § 103(a) as unpatentable over Fielder as applied to claim 1, and further in view of Menezes (Handbook of Applied Cryptography).

C. Claims 2-4 were rejected under 35 U.S.C. § 103(a) as unpatentable over Fielder as applied to claim 1, and further in view of Yatsukawa (U.S. Patent No. 6,148,404).

D. Claims 10 and 13 were rejected under 35 U.S.C. § 103(a) as unpatentable over Fielder and Menezes as applied to claim 1, and further in view of Lamport, Leslie (Password Authentication with Insecure Communications).

VII. Argument

A. Claims 1, 5-8 and 16-19 under 35 U.S.C. § 102(e) as anticipated by Fielder: Fielder does not teach the claim element that "the server device sends update data to the client device."

To render a claim unpatentable under 35 U.S.C. § 102, a cited reference must disclose each and every limitation in the claim. *Verdegaal Bros. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987); *see also* MPEP § 2131. Claim 1 recites in part "the server device sends update data to the client device." Fielder does not disclose this claim limitation (see Section B below for a more complete discussion). In fact, the Office Action itself states that this is the case. On page 7 lines 11-12, the Office Action states that Fielder discloses certain claim limitations "but failed to disclose the change value being received from the answering system." According to the Office Action, Fielder's "change value" corresponds to claim 1's "update value" and Fielder's "answering system" corresponds to claim 1's "server device." Thus, by the Office Action's own admission, Fielder does not disclose each and every limitation in claim 1. This reasoning applies equally to independent claims 18 and 19 since these claims both contain the same limitation. Hence, claims 1, 5-8 and 16-19 are patentable over Fielder.

B. Claims 1, 5-8, 11-12 and 14-19 under 35 U.S.C. § 103(a) as unpatentable over Fielder and Menezes: Fielder does not teach that "the server device sends update data to the

client device." In fact, Fielder expressly teaches that the server device does NOT send update data to the client device and, therefore, even if Menezes taught this element, modifying Fielder to achieve the claimed invention would render Fielder's system unsuitable for its intended purpose.

Even assuming that Menezes teaches the claim limitation that "the server device sends update data to the client device," it would not have been obvious to one of skill in the art to modify Fielder in light of Menezes to achieve the claimed method. This is because such a modification would destroy a fundamental principle of operation of Fielder. In making an obviousness rejection, an examiner cannot propose a modification that renders the prior art unsatisfactory for its intended purpose. *In re Gordon*, 733 F.2d 900 (Fed. Cir. 1984); MPEP § 2143.01. Because the Office Action seeks to modify Fielder in a way that destroys Fielder's fundamental principle of the server device NOT sending update data to the client device, the proposed combination is improper.

The primary issue is whether the server device NOT sending update data to the client device is a fundamental principle of Fielder. Appellant contends that it is a fundamental principle, for the reasons given below. The Office Action contends that it is one embodiment of Fielder but is not a fundamental principle.

More specifically, Appellant believes that the server device NOT sending update data to the client device is a fundamental principle of Fielder for three main reasons:

1. Fielder's disclosure repeatedly and broadly emphasizes the importance of NOT sending update data between the devices in order to increase security.

2. Appellant could not find a single example or suggestion that Fielder ever contemplated an embodiment where update data is sent between the devices.

3. Appellant could not find the passage that is relied on in the Office Action. The quotation that is allegedly from Fielder's abstract does not appear in the abstract for 5,995,624, which is the patent identified as the Fielder reference.

In more detail, taking claim 1 as an example, claim 1 concerns validating a client device by a server device through use of a shared unpredictable secret. One step involves replacing the shared unpredictable secret. Specifically,

"the server device sends update data to the client device;

the client device applies the update data to the shared unpredictable secret to generate a new secret; and

the client device replaces the shared unpredictable secret with the new secret."

Claim 1 expressly recites that the server device sends update data to the client device. This feature is beneficial because it allows a client device to generate a new secret based on update data sent by the server device.

The Office Action compares Fielder to the claimed invention, stating that Fielder's "originating system" corresponds to claim 1's "client device," that Fielder's "answering system" corresponds to claim 1's "server device" and that Fielder's "change value" corresponds to claim 1's "update data." Thus, according to the Office Action, the claim 1 limitation of "the server device sends update data to the client device" would be met by a showing that Fielder's answering system sends a change value to the originating system. The Office Action goes on to state that while Fielder discloses that the originating system applies a change value to the dynamic secret in order to update the secret, Fielder fails to disclose that the answering system sends the change value to the originating system. Office Action, page 7 lines 11-12. The Office

Action then goes on to state that Menezes discloses this missing limitation and, therefore, claim 1 is rejected in light of the combination of Fielder and Menezes.

Regardless of whether the combination teaches all the elements of claim 1, the combination of Fielder and Menezes itself is not proper. Fielder expressly and repeatedly states that the change value is not sent from one device to the other, thus preventing discovery of the change value during the sending. For example (emphasis added):

> In Fielder's Abstract: "An authentication and information encryption system and method which uses a token system for increased security in accommodating bilateral encrypted communications between an originating system and an answering system, with each system without synchronization independently generating a message digest through use of an encryption key generator which employs bit-shuffling, many-to-few bit mapping, and secure hash processing to forestall attempts to discover the secret inputs to the generator, or the system password, encryption key, or change value outputs extracted from the message digest, through cryptographic analysis or brute force trial-and-error attacks, and with each system using the passwords, encryption key and change value during only a single system connection before using the change value to update one of the secret inputs to the key generator to provide new password, encryption key and change value parameters having no predictable relationship to their previous counterparts, and with each system accommodating plural authentication cycles to verify the originating system, the answering system, the token system, and the pairing of the token system with either the originating system, the answering system, or both, all without public exposure of the secret inputs, encryption key or change value
>
> In Fielder's Summary (3/16-3/34): "In accordance with the present invention, bilateral authentication of an originating system, an answering system, and an originating system/token system pair occurs, and the encryption of information to be exchanged between the originating system and the answering system occurs, without exposing data other than system identifiers.
>
> In one aspect of the invention, a static secret and a dynamic secret initially are known by the originating system and the answering system, but are never revealed by one system to the other. The systems independently use such secrets to generate message digests from which system passwords, a secret session encryption key, and a change value are extracted, and information encrypted with the secret session encryption key is exchanged between the systems without need for the secret session encryption key or the change value to be exposed in any form, or for the system passwords to be exposed in other than encrypted form."
>
> With respect to Fielder's FIG. 1 (6/51-7/9): "In accordance with the invention, both computer system 10 and computer system 11 have a unique plural bit identifier which is stored on their respective hard disk drives, and which may be exchanged by the computer

systems in cleartext. The identifiers may be comprised of numerics and/or text. The static secret is known by each system, but is not exchanged over the communication link. The static secret never changes unless the current value is purposely overwritten with a new value.

A dynamic secret also is shared by the two computer systems, and held in confidence, and never transmitted over the communication link 12. The secret is dynamic in the sense that each time a bilateral authentication of the computer systems occurs, the dynamic secret is altered. The change value that is used is a pseudo-random number. As will be explained in more detail below, the dynamic secret makes the cryptographic result of the encryption key generator unpredictable without knowledge of both the static secret and the dynamic secret. As one aspect of the invention, the change value is not made part of any access request or information that is exchanged between the computer systems. Thus, the change value is not subject to discovery as a result of information communicated over the communication link 12.

It is to be understood that the static secret, the dynamic secret, the change value, and the session encryption key are never communicated out from the computer system in which they are generated and stored."

Later in the same explanation (7/40-7/45): "For purposes of the invention, the message digest 24 is divided into four sectors. The first sector is an originating system password 25 which is used one time, the second sector is an answering system password 26 which also is used one time, the third sector is a secret session encryption key 27, and the fourth sector is a change value 28. The contents of each of the sectors comprising the message digest are pseudo-random numbers, which each of the computer systems 10 and 11 have produced independently without need for synchronization. Thus, computer system 10 has its own one-time password and knows the one-time password for the computer system 11. Further, each has the secret session encryption key 27 without any exchanges other than system IDs over a communication media."

The Office Action contends that while in some embodiments, the answering system does not send the change value to the originating system, this is not a fundamental principle of operation for Fielder and, therefore, in other embodiments, the answering system could send the change value to the originating system. The Office Action draws this conclusion because "[t]he principle of operation of Fielder is clearly expressed in the first five lines of the abstract as being 'a bilateral system for authenticating remote transceiving stations through use of station identifiers (Ids), and through use of passwords which are used only one time, and thereafter exchanging messages through use of an encryption key which is changed after each system connection.'" Office Action, page 2 line 14. However, this is puzzling because this passage

does not appear to be drawn from Fielder's abstract. Fielder's abstract is reproduced in part above and clearly states that the two devices operate independently of each other and there is no exchange of the change value. Furthermore, Fielder's summary repeats this principle of operation, as does Fielder's background and Fielder's description of preferred embodiments. In fact, Appellant could not find a single passage in Fielder that states, or even suggests in any way, that the change value is sent from one device to the other, let alone from the answering device to the originating device.

Therefore, Appellant respectfully submits that it is a principle of operation of Fielder that the change value is NOT sent between the two devices. Accordingly, Fielder cannot be properly combined with a reference that teaches exactly the opposite. It is well established that a combination of prior art is improper if the combination would change the principle of operation of a reference. M.P.E.P. § 2143.01, citing *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). In this case, the alleged combination of Fielder and Menezes would require sending the change value between Fielder's devices, which would change Fielder's basic principle that the change value is NOT sent between the devices. Similarly, references are not properly combinable if their intended function is destroyed. M.P.E.P. § 2143.01, citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). In this case, the alleged combination would destroy Fielder's intended function of encrypted communication without sending the change value from one device to the other.

For at least this reason, claims 1, 5-8, 11-12 and 14-19 are patentable over Fielder and Menezes.

C. Claims 2-4 under 35 U.S.C. § 103(a) as unpatentable over Fielder and Yatsukawa.

The remarks made in Section B above apply equally to this ground of rejection. Fielder does not teach that "the server device sends update data to the client device." In fact, Fielder expressly teaches that the server device does NOT send update data to the client device and, therefore, even if Yatsukawa taught this element, modifying Fielder to achieve the claimed invention would render Fielder's system unsuitable for its intended purpose. Therefore, claims 2-4 are patentable over Fielder and Yatsukawa.

D. Claims 10 and 13 under 35 U.S.C. § 103(a) as unpatentable over Fielder, Menezes and Lamport, Leslie.

The remarks made in Section B above apply equally to this ground of rejection. Fielder does not teach that "the server device sends update data to the client device." In fact, Fielder expressly teaches that the server device does NOT send update data to the client device and, therefore, even if Menezes or Lamport, Leslie taught this element, modifying Fielder to achieve the claimed invention would render Fielder's system unsuitable for its intended purpose. Therefore, claims 10 and 13 are patentable over Fielder, Menezes and Lamport, Leslie.

Summary

For the foregoing reasons, Appellant believes that the examiner's rejections of claims 1-8 and 10-19 were erroneous, and reversal of his decision is respectfully requested.

Respectfully submitted,

Dated: January 22, 2007

By: /Michael W. Farn/

Michael W. Farn, Reg. No. 41,015
Attorney for Appellant
Fenwick & West LLP
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7823

Appendix: Claims Involved in Appeal

1. A method for validating a client device by a server device, said method comprising the steps of:

generating a shared unpredictable secret;

storing the shared unpredictable secret in the client device and in the server device;

requiring the client device to prove that it holds a correct secret as a precondition to the server device validating the client device; and

replacing the shared unpredictable secret by a new shared unpredictable secret when the server device validates the client device, wherein:

the server device sends update data to the client device;

the client device applies the update data to the shared unpredictable secret to generate a new secret; and

the client device replaces the shared unpredictable secret with the new secret.

2. The method of claim 1 wherein an initial shared unpredictable secret is determined in the client device and in the server device during a registration step that occurs prior to a log-in step.

3. The method of claim 2 wherein the registration step entails more checking of authentication data presented by the client device than does the log-in step.

4. The method of claim 2 wherein, during the registration step, the client device is required to make a payment to the user device.

5. The method of claim 1 wherein the shared unpredictable secret is generated by a generator from a group comprising a random number generator and a pseudo-random number generator.

6. The method of claim 1 wherein the shared unpredictable secret comprises an unpredictable component and a fixed component.

7. The method of claim 1 wherein a plurality of client devices desire to be validated by the server device; and each client device has a unique unpredictable secret that it shares with the server device.

8. The method of claim 1 wherein, following a validation of the client device, the server device discards the shared unpredictable secret and stores within the server device the new shared unpredictable secret that can be generated by applying the update data to the shared unpredictable secret.

10. The method of claim 1 wherein:

the server device generates the update data using a generator from a group comprising a random number generator and a pseudo-random number generator; and

the step of applying the update data to the shared unpredictable secret comprises computing a one-way function of a combination of the shared unpredictable secret and the update data.

11. The method of claim 1 wherein the client device sends acknowledgement data to the server device to confirm that the client device has replaced the shared unpredictable secret with the new secret.

12. The method of claim 11 wherein, in response to the server device receiving the acknowledgement data from the client device, the server device:

validates the client device; and

discards the shared unpredictable secret and stores within the server device the new secret, which now becomes the new shared unpredictable secret.

13. The method of claim 11 wherein:

the client device sends to the server device proof data demonstrating that the client device holds the correct secret; and

the server device is adapted to accept from the client device any proof data that are generated from a secret that is newer than the secret for which the most recent acknowledgment data have been received by the server device.

14. The method of claim 11 wherein:

the client device sends to the server device both the acknowledgment data and proof data derived from the new secret.

15. The method of claim 14 wherein:

the proof data are computed on the new secret; and

the proof data serve also as the acknowledgment data.

16. The method of claim 1 wherein:

the client device presents proof data to the server device, wherein the proof data are derived from the shared unpredictable secret using a proof data generation algorithm, and the proof data do not divulge the shared unpredictable secret;

the server device checks the proof data by using a proof data generation algorithm consistent with the proof data generation algorithm used by the client device; and

when the server device determines that the proof data presented by the client device were not generated from the shared unpredictable secret that is stored in both the client device and in the server device, the server device does not validate the client device.

17. The method of claim 16 wherein each proof data generation algorithm is a one-way function.

18. A system for enabling a server device to validate a client device, said system comprising:

at least one client device;

a server device;

a shared unpredictable secret;

means for storing the shared unpredictable secret in the client device;

means for storing the shared unpredictable secret in the server device;

coupled to the client device and to the server device, means for determining whether the client device holds a correct secret;

coupled to the determining means, means for allowing the server device to validate the client device when the client device proves that it holds a correct secret; and

coupled to the client device and to the server device, means for replacing the original shared unpredictable secret with a new shared unpredictable secret when the server device validates the client device, said means for replacing further comprising:

means for the server device to send update data to the client device;

means for the client device to apply the update data to the shared unpredictable secret to generate a new secret; and

means for the client device to replace the shared unpredictable secret with the new secret.

19. A computer readable medium containing computer program instructions for enabling a server device to validate a client device, said computer program instructions causing the execution of the following steps:

generating a shared unpredictable secret;

storing the shared unpredictable secret in the client device and in the server device;

requiring the client device to prove that it holds a correct secret as a precondition to allowing the client device to be validated by the server device; and

replacing the shared unpredictable secret by a new shared unpredictable secret when the client device is validated by the server device, wherein:

the server device sends update data to the client device;

the client device applies the update data to the shared unpredictable secret to generate a new secret; and

the client device replaces the shared unpredictable secret with the new secret.

Evidence Appendix

None.

Related Proceedings Appendix

None.